## **PCT**

## WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau



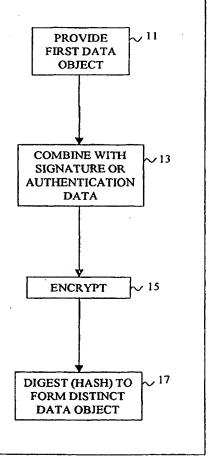
### INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> :		11) International Publication Number: WO 00/1336
H04L 9/32	43) International Publication Date: 9 March 2000 (09.03.00	
(21) International Application Number: PCT/US (22) International Filing Date: 27 August 1999 (		(81) Designated States: CA, IL, IN, JP, KR, MX, European pater (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, I' LU, MC, NL, PT, SE).
<ul> <li>(30) Priority Data: 09/144,043 31 August 1998 (31.08.98)</li> <li>(71)(72) Applicant and Inventor:</li></ul>	(US). ) Renai	Published  With international search report.  Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt amendments.

#### (54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

#### (57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



# MENT OF THE PROPERTY OF PROPERTY OF THE PARTY OF THE PART

## MOOTHS TO ELECTION OF THE PARTY OF THE PARTY

O production of the content of the complete of the providing of the content of th

## ERA BATOMINGAG GRAA MODIMIETA JOHARA ERA JOHANA

The state of the s

The MARGO BURE TO ARE IT TO STELLED A INTERPORT OF ADMINISTRATION OF A AREA OF THE

		sode is	ligib i	FOR THE PURPOSES O	OF INF	ORMATION ONLY	re prije gr	rge "
								applications under the PCT
	AL AM AT AU	Albania Armenia	ES FI	Spain Finland France	LS.	Lesotho Lithuania	SK	Slovenia Slovakia Senegal Swaziland
	AZ BA	Azerbaijan Bosnia and Herzegovina	GB GE	United Kingdom	MC MD	Monaco Republic of Moldova	TD	Chad
. :	BE BE	Barbádos (1. (2.1) (3.2) (3.2) Belgium Burkina Faso	GN	Guinea	MG: J MK	Madagascar 11, 12, 13, 14, 14, 14, 14, 14, 14, 14, 14, 14, 14	TM	Turkmenistan
1	BG. (C)	Bulgaria Benin	GR HU IE	Greece Hungary Ireland	ML.	Republic of Macedonia Mali Mongolia	TT	Turkey Trinidad and Tobago Ukraine
	BR BY.	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
;	CA	Belarus Canada	is IŤ. '' :	Iceland Italy	MW	Malawi Mexico	US	United States of America Uzbekistan
	CF CG	Central African Republic Congo	JP	Japan	NE	Niger	VN	Viet Nam
- 5	CH (L)	Switzerland Côte d'Ivoire	KE KG KP	Kenya Kyrgyzstan Democratic People's	NL NO NZ	Norway 12 20 New Zealand	YU Mag <b>Z</b> W.o.q.	Yugoslavia Zimbabwe
٠.		Cameroon China Cuba		Republic of Korea Republic of Korea Kazakstan	PL	Poland Portugal Romania	•	
l	.CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation	•	
		Germany	LI	Licchtenstein	SD	Sudan		
		Denmark	LK	Sri Lanka	SE	Sweden		
	EE	Estonia	LR	Liberia	SG	Singapore		
				•				

WO 00/13368 PCT/US99/18824

# METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

## TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to providing authentication of digital data, such as document or other data files or objects. More particularly, the present invention relates to methods of securely appending or otherwise incorporating a digital signature or indicia of authenticity into a data object.

## BACKGROUND OF THE INVENTION AND BACKGROUND ART

There have been several prior attempts to digitally "sign," "notarize," or otherwise authenticate a digital data object such as a text document. Generally speaking, one drawback to the storage of, for instance, digital document files, is that it can be difficult to establish whether the version retrieved or transmitted is the identical document originally stored or created. A "digital signature" or "notary" is a common nomenclature for an attempt to provide indicia of authenticity of the digital data.

One such method is found in U.S. Patent Number 5,022,080, June 4, 1991, to Durst et al., which discloses a method of digitally notarizing a document comprising the steps of hashing the document, transmitting the digest (or result of the hash) to a trusted third party, where the digest is combined with a time-stamp, and then encrypting the combination to produce a "digitally notarized" document. All that is required to authenticate the document is the key to the encryption technique. Thus, simply by "breaking the code" the authenticity indicia or the underlying data object can be altered

or tampered with.

。明明的感觉,4、一直,2年,2年,2年页**线键** 

Other solutions complicate this basic scheme to render it more difficult to break the code successfully. For instance, U.S. Patent Number 5,373,561, December 13, 1994 to Haber et al., periodically re-encrypts the signature data to take advantage of ever-increasing computational power and advances in encryption, which also render the authentic document more susceptible to alteration, decryption, or tampering as time passes. However, if the user neglects to update, the encryption, the advantage is lost. A need exists, therefore, for a method of digitally authenticating a data object that is not susceptible to future tampering, yet is sufficiently simple as to be implemented in a practical and efficient manner.

The first constitution of the section of the sectio

Addition of Expendence of the second of the

建氯铁矿 高电压 神经 化二烷

## DISCLOSURE OF THE INVENTION

It is a general object of the present invention to provide a method of providing a data object that can ve verified or authenticated reliably, with minimal risk of tampering.

This and other objects of the present invention are achieved by associating or combining a data object, such as a document file, with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated or digested from the combination of encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data.

According to the preferred embodiment of the present invention, the generation of the distinct data object is achieved using a hashing algorithm, such as SHA-1.

According to the preferred embodiment of the present invention, the signature or authentication data is provided by a trusted third party. The data object transmitted to the third party may be a digest or hash of the data object to preserve the confidentiality of the data object.

According to the preferred embodiment of the present invention, the encryption step is achieved by a symmetric encryption algorithm.

According to the preferred embodiment of the present invention, the authenticity of the original data object is confirmed by reproducing the distinct data object by identically encrypting a data object identical to the original, generating another distinct data object, and comparing the second and first distinct data objects for identity.

-- ;, --

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a high-level flow chart depicting the steps of the method according to the preferred embodiment of the present invention, and more particularly the steps of proving a data object with authentication of signature data.

Figure 2 is a block diagram schematically depicting a portion of the method of Figure 1 according to the preferred embodiment of the present invention. 10 1 march 10

Figure 3 is a high-level flow chart illustrating the steps of the method according to the preferred embodiment of the present invention, and more particularly of the steps of authenticating a data object provided with authentication data.

Figure 4 is a block diagram schematically depicting a portion of the method of

Figure 3 according to the preferred embodiment of the present invention.

to history in the professional contract the profession of the guingment with the and the state of the section is not be also which the contract of the section of and the first boursaning of the late of an All of money which profession are clayed this man are to go of 2.15 for 4 April 1995. The signature of the archimiller au ro Bomisia du Mariana cama palemente de la comissión de la la comissión de la comisisión de la comissión de la comissión de la comissión de la comis may a manada fi erugida e uma dikara da kinak mesengi dia kinak da maka yang Survey for group being bors of a 14 to 1, to the late of the late to be seen we are suggested to tandar er sem er tibaltom selt a mer er mankatting sem of estimaterija alter men betyden. end with conscious a source good a region seed that there is

electic design force resido constante inconcineramos coltante prepara que grande coltante de la coltante de la and selection does in encomplet estate conventional everyone secretisky largereness.

## MODE(S) FOR CARRYING OUT THE INVENTION

Referring now to the Figures, and specifically to Figure 1, a high-level flow-chart depicts the basic steps of a portion of the method according to the present invention.

First, at block 11, a first data object or item is provided by a user or customer of the

the description method. The data objection item could be a document, drawing, image file, or any item

or segment of data that the user desires to provide with the ability to be authenticated or

La broom tverified in the future of gring audit made word level-rigid nated many

authentication data. The signature or authentication may include the time of creation of the data object, the name of the author of the object, predetermined characters indicating the origin of the object, or virtually any other data the user desires to serve as evidence of authenticity of the underlying data object. According to the preferred embodiment of the present invention, the authentication data is a "time stamp" that comprises, for instance, the time and date from the "Atomic Clock" maintained by the United States Naval Observatory (e.g., 22:13.02; 4 April 1998). The signature or authentication data is appended, concatenated, or otherwise conventionally combined or associated with the data object. As discussed in greater detail with reference to Figure 2, the time stamp or other signature or authentication data is provided by a trusted third party, perhaps the vendor of the method, who also keeps meticulous records of the method used to combine or associate the data object with signature or authentication data.

Next, at block 15, the combination of the data object and signature or authentication data is encrypted using conventional symmetric secret-key, asymmetric

#### WO 00/13368

1. XX 医自己 人名英格兰

: 1. 0

public-key techniques or other combining techniques which use a key known only to the trusted third party. The encryption technique could be as simple as appending or concatenating a selected, random text or character string to the data object. For maximum security, it is preferable that the trusted third-party employ secret-key techniques and maintain a record of the encryption technique along with any secret-keys, for future use in authentication of the data object. The preferred encryption method or algorithm is obles to a recipient purry, o permit the recipion party to later condi-

Finally, at block 17, the encrypted data object is digested or hashed using a hash routine to generate a distinct data object. A hash routine generates a data string that is characteristic of the underlying data object that is subjected to the hash routine. The preferred hashing algorithm is SHA-1. There are several hashing routines or algorithms, such as SHA-1, that are suitable for use in the method according to the present invention. All of these hashing routines or algorithms share the following characteristics:

- the underlying data object cannot be reproduced from the hashed data string (it is a one-way of irreversible process); . Subcading
- the routine produces a data string of fixed length; and
- the routine will not yield the same data string for two different data objects. Hashing is sometimes referred to as a method of encryption, but this is inaccurate: the very essence of encryption is that it can be decrypted or the process reversed. Hashing, by its very nature, is not reversible. According to the preferred embodiment of the present invention, the hashing or digesting step may comprise application of a single hashing algorithm or routine to the encrypted data object and signature data.

STUATION.

· :;

Alternatively, the hashing step may comprise multiple applications of the same or

The result of the hashing step is a distinct data object that has characteristics of both the underlying data object and the signature or authentication data. The distinct data object may be appended to or separate from the underlying data object. The distinct data object and the signature or authentication data is transmitted, along with the original data object to a recipient party to permit the recipient party to later confirm the authenticity of the original data object and/or the combination of the data object and the signature or authentication data is transmitted.

performing the steps of the method according to the present invention. According to the preferred embodiment of the present invention, the encryption and hashing steps are performed on the user's computer 19 which may be a personal computer, a client/server workstation, terminal for a mainframe or minicomputer or the like. The signature or authentication data is provided by a trusted third party 21, who also provides the encryption and hashing algorithms and keeps a record of the encryption or combining techniques and any secret keys for use in future authentication. Alternatively, the encryption and hashing algorithms are resident on and maintained by user's system 19.

According to one embodiment of the invention, the original data object is hashed and then sent to the trusted third party 21 to preserve the confidentiality of the original data object. In this embodiment, the trusted third party performs the encryption and hashing or digesting steps and returns the resulting distinct data object and authentication

3. 数10 · 15 · 11 · 15 \$

data to user 19 to associate with or combine with the original data object.

Communication between user 19 and trusted third party 21 is accomplished in a number of ways: through modem line, T1 line, frame relay link, or cable modem, or http protocol (each with appropriate security). Trusted third party 21 maintains records of any encryption keys, the encryption technique and hashing algorithm(s) for future use by the party that later performs authentication of the document.

Figure 3 is a high-level flow chart-depicting the steps of the authentication portion of the method according to the present invention. To authenticate the data object, an original copy, block 31, of the data object, identical to the first, is combined with signature or authentication data, at block 33. The original copy of the data object and signature or authentication data can be provided by the originator, or can be kept by the trusted third party along with the encryption and/or hashing algorithms. After the copy of the original data object is combined with the authentication or signature data, the combinations is encrypted in an identical fashion to the original, at block 35. At block 37, the resulting encrypted data object is then hashed or digested identically to the first, and the resulting distinct data object compared with the original data object (the result of block 17 in Figure 1) and the two are compared for identity. If the two are identical, the than by all had be at the change of the underlying data object (or the copy) is thus verified or authenticated. If not identical, the 其心,所以其中,以上於一致如此無效。 表示的 网络一种人 data object or copy is not authenticated and cannot be trusted (i.e., the copy or document purporting to be original has been altered and is not identical to the first or the authentication data has been altered).

Figure 4 is a block diagram depicting elements and relationships between entities

performing the steps of the authentication portion of the method according to the present invention. According to the preferred embodiment of the present invention, the authentication steps/are performed by a trusted party, perhaps the vendor of the method the back the recipient party 25 using information provided by the trusted third party, the originator or user, or a combination of the two. The distinct data objects are input to a comparator or a computer algorithm operable to compare data for identity. The output of the comparator verifies the authenticity (or lack thereof).

According to the preferred embodiment of the present invention, the method is performed using software resident on the document or data object originator's computer. The encryption and digesting occurs on the trusted third party's computer with the input and results being communicated to and from the trusted third party as described above. The recipient of the "authenticated" data object can request verification through the trusted third party; depending upon which of the parties maintains the requisite encryption technique, hashing algorithm, combination method, and any encryption keys.

9 . S

white agreement of

The method according to the present invention provides an improved method of digitally signing or otherwise authenticating digital data objects. Because the hashing or digesting step is one-way or irreversible, the encrypted portion of the "signature" is not susceptible to unauthorized decryption, even by marked advances in computational Selver a prior for petron by aniplotonia power. Because of this advantage, the trusted third party or vendor must keep scrupulous records of the encryption or combining techniques, hashing methods and encryption keys Law of 150 ha to the star graying employed in providing the signature or authentication data. The trie is a section to releasification

The invention has been described with reference to preferred embodiments thereof.

#### WO 00/13368

It is thus not limited, but is susceptible to variation and modification without departing from the scope and spirit of the invention, which is defined by the claims, which follow.

e com al qualitie object out algorithm distribution

- com and algorithm days object from the agreement form of the compact of

in the oding distinct and the distinct constituent of the state of the second section of the section of the second section of the second section of the second section of the section of the second section of the sect

and the second problem is the second problem of the second problem of the second problem is a second problem of the second problem is a second problem of the second problem in the second problem is a second problem of the second problem in the second problem is a second problem.

The common section was an experienced by the property of galactic and quantum of the control of the analysis of the control of

The control of the second for the form of the control of the contr

The medical man of the defend on a second sequences downs processed by the control of the contro

3 is particular data encryption is integred, where it is in integrated by professional and will in a substitution of ata encryption is integred.

## Supremo (CLAIMS) of the Common of a of shifting we are not find from the land of all

1. A method of securely associating signature data with other data, the method isolar a choosel of the dide talk on the editions: comprising the steps of:

associating a data object with signature data;

encrypting both the data object and the signature data; and

generating a distinct data object from the encrypted data object and signature data, the distinct data object having characteristics determined by the data object and the signature data.

- 2. The method according to claim 1 further comprising the step of: delivering the distinct data object and signature data to a recipient party.
- 3. The method according to claim 2, further comprising the step of: validating the distinct data object and signature data combination by:

associating a second data object, identical to the first, with the signature data;

encrypting the second data object and the signature data using an encryption method identical to that employed in encrypting the first data object and the signature data;

generating a second distinct data object from the encrypted second data object and the signature data using an method identical to that employed in generating the distinct data object; and

comparing the distinct and second distinct data objects for identity.

- 4. The method according to claim 1, wherein the signature data is provided by a trusted party.
- 5. The method according to claim 1, wherein the encrypting step is performed using a symmetric data encryption technique.

- ' ' ( ,

17. 115

- 6. The method according to claim 1, wherein the step of generating the distinct data one in the commence of object is performed using a hash routine.
- 7. A method of providing a time-stamp for a data object comprising the steps of: generating a distinct value for the data object; associating signature data with the distinct value to produce a signed data object; encrypting the signed data object; and seems me as guissing a

generating a second distinct value from the encrypted signed data object, the second distinct data object having characteristics of the encrypted signed data object. generating a scood distinct value from the copypted ancewers in one or

- 8. The method according to claim 7 further comprising the step of: delivering the second distinct data object and signature data to a recipient party. were sit subliqued in 1975 to also of a finary had a cold in.
- 9. The method according to claim 8, further comprising the step of: validating the second distinct data object and signature data combination by: generating a third distinct value, identical to the distinct value; associating a second signature data, identical to the first, with the third distinct value to produce a second signed data object; and

encrypting the second signed data object using an encryption method identical to that employed in encrypting the first signed data object;

generating a fourth distinct value from the encrypted second signed data object using method identical to that employed in generating the second distinct " walue: and " " it is The state of the Country of

comparing the fourth distinct value and second distinct value for identity. e let e let est este le relateir l'albane face e deveniment d'una ès it gripagnes à

- 10. The method according to claim 7, wherein the signature data is provided by a trusted is bus party. The section without the two of quelongers on a referred wi
- 11 The method according to claim 7, wherein the encrypting step is performed using a symmetric data encryption technique.

· 以注意,以图[[]、WO 00/13368

The method according to claim 7, wherein the step of generating the distinct value is performed using a hash routine. combined describe union become consistence.

2. 13. A method of providing a time-stamp for a data object comprising the steps of: generating a distinct value for the data object by performing a hash routine on the is fide a data, object; which is the standard with the standards and brons a associating a time-stamp with the distinct value to produce a time-stamped data

object; there some were all most only their in backer is gained and encrypting the time-stamped data object; and and bound for the control of the generating a second distinct value from the encrypted time-stamped data object by performing a hash routine on the encrypted time-stamped data object.

14. The method according to claim 13 further comprising the step of: delivering the second distinct data object and time-stamp to a recipient party.

Province and a larger box was a state contain teacher of action for

in the strapped will be the comparate that the property of the property of the comparate control of the

nga kita nga <mark>nge</mark>rapida.

15. The method according to claim 13, further comprising the step of: validating the second distinct data object and time-stamp combination by: generating a third distinct value, identical to the distinct value; associating a identical time-stamp with the third distinct value to produce a second time-stamped data object on a tomar salt of faction be encrypting the second time-stamped data object using the identical

encryption method; and the harmonic in the manufacture of the second sec generating a forth distinct value from the encrypted second time-stamped the second data object; and the second and which if the consumer of the second

comparing the fourth distinct value and second distinct value for identity.

16. The method according to claim 13, wherein the time stamp is provided by a trusted party.

Albertaer de la la marce charge en l'arbet et abbiologique bollogisté de

ng sanbanca ng a galapatgyana na malah Nabab at yang dalah at tidak at galam da babbat si Hilli. U

- . . .

17. The method according to claim 13, wherein the encrypting step is performed using

a symmetric data encryption technique.



Mark Congression Streets Constitution Market Constitution using 1/4 and leastly least the instruction of

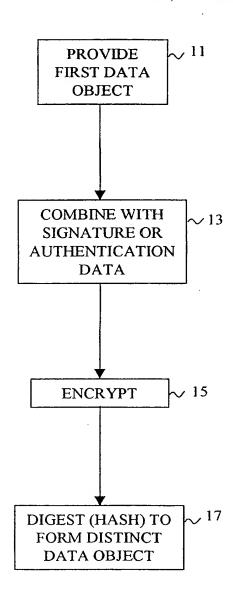


FIG. 1

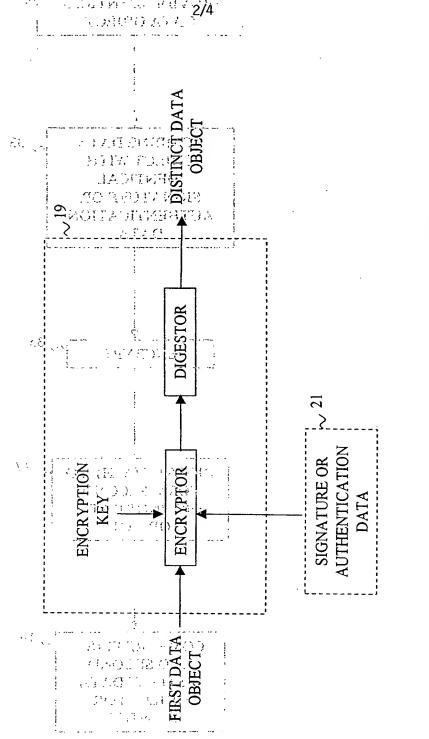


FIG. 2

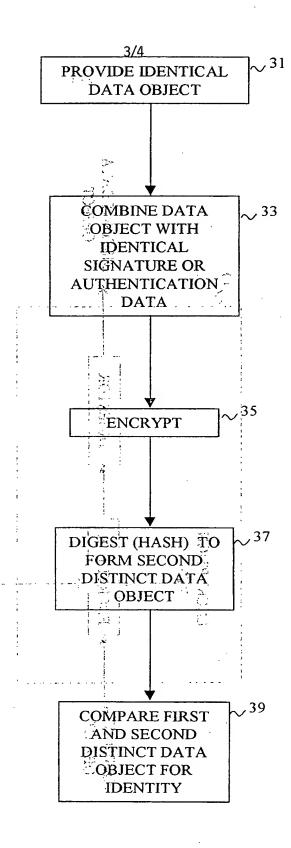
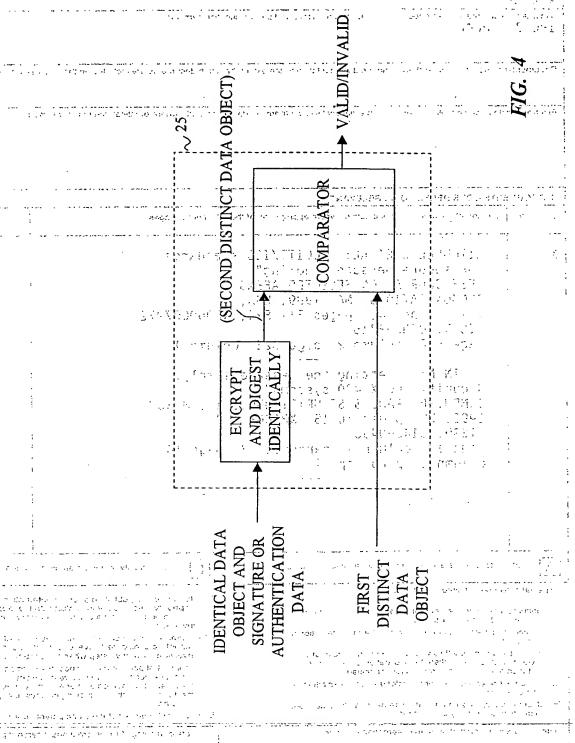


FIG. 3

H. 18.7 .



WELL HALL

Spel dedutions you

1

## INTERNATIONAL SEARCH REPORT

Inter anal Application No PCT/US 99/18824

7 1/ 1/ 1 1		7.1.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7	7,6000.
	FICATION OF SUBJECT MATTER H04L9/32		
According t	o International Patent Classification (IPC) or to both national classifi	cation and IPC	
B. FIELDS	SEARCHED		
Minimum de IPC 7	ocumentation searched (classification system followed by classifical HO4L	tion symbols)	·
1,0 /	90 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -		
Cocumenta	tion searched other than minimum documentation to the extent that	Cuch door and a second of the first	
Ç.;	Section of Street Walt Manufacture and Section (1997)	aden documents are included in the helds se	earched
e *15	lata base consulted during the international search (name of data).		
Liectionic	and base considered during the international search thanks of data.	ase and, where practical, search terms used	)
	An .		
	·	i	·
	CHTC CONCIDENCE TO AS OF STATE OF		
Category	ENTS CONSIDERED TO BE RELEVANT  Citation of document, with indication, where appropriate of the ra	Novant raceanes	Onle serve ele es No
oursgo.,	ordinary actions. Where appropriate, of the ra	nevan passages	Relevant to claim No.
х	MITCHELL C ET AL: CCITT/ISO st	andards	1-17
	for secure message handling"; 🔄		1 1,
	IEEE JOURNAL ON SELECTED AREAS TO COMMUNICATIONS, MAY 1989, USA,	N ·	
	vol. 7, no. 4, pages 517-524, X	P000007972	·
	ISSN: 0733-8716	:	
	page 520, column 2 -page 522, co	lumn 1:	
х	SWAIN N: "Getting the message s	afely.;	1-17
	Security and X.400 systems" COMPUTER FRAUD & SECURITY BULLET	TN MADCH	•
	1992, UK, pages 10-15, XP0008629	48	
	ISSN: 0142-0496		
	page 13. column 1. paragraph 3 - column 1. paragraph 1	page 14.	
		-/	
		·	
X Funth	ier documents are listed in the continuation of box $C^{\infty}$ . $\mathbb{C}$	Patent family members are listed in	n annex.
Special cat	legories of cited documents		
	nt defining the general state of the art which is not 🤼 👵 🥳	"I alter document published after the intension or priority date and not in conflict with the cited to understand the principle or the	he application but
"E" earlier d	ered to be of particular relevance (in the international in the international i	invention "X" document of particular relevance; the cla	
filing da "L" docume	nt which may throw doubts on priority claim(s) or	cannot be considered novel or cannot to involve an inventive step when the doc	pe considered to
citation	s cited to establish the publication date of another or other special reason (as specified)	"Y" document of particular relevance; the ck cannot be considered to involve an inve	aimed invention entive step when the
other n		document is combined with one or mor ments, such combination being obvious	e other such docu-
later th	nt published prior to the international filing date but an the priority date claimed	in the art. "%" document member of the same patent fa	amily
Date of the a	ictual completion of the international search	Date of mailing of the international sear	ch report
1 7	7 December 1999	21/01/2000	
	nailing address of the ISA	Authorized officer	
	European Patent Office. P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk	Addionated Officer	
	Tel. (+31-70) 340-2040. Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	. Zucka, G	

1

# INTERNATIONAL SEARCH REPORT

Inter anal Application No

		PCT/US 99/18824					
	ation) DOCUMENTS CONSIDERED TO BE RELEVANT	2.00					
Category	Citation of document, with indication where appropriate of the relevant passages	Part	Relevant to staim No				
X	US 5 022 080 A (DURST ROBERT T ET AL) 4 June 1991 (1991-06-04) cited in the application column 3 1 ine 65 -column 6, line 54  US 5 373 561 A (HABER STUART A ET AL) 13 December 1994 (1994-12-13)	2 10 10	1-17				
X	US 5 638 446 A (RUBIN AVIEL D) COLUMN 12, 13 ine 38 -column 6. line 44  US 5 638 446 A (RUBIN AVIEL D) COLUMN 10 June 1997 (1997-06-10)  column 3, line 49 -column 6, line 20		1-17				
			:				
n	······································						
			: 				
	·						

• •:	; 1				NATION rmation on p				* * * * *		ter on				
	$\beta_2 \leq$	<del></del>	<u> </u>		· · · · · · · · · · · · · · · · · · ·						CT/US		<del></del>		
7 77 10	Pa Juleo	itent d	document earch repor	t. 		date	BANK Tabu	PER SE P	Patent fa member	mily `	seria es		Public	cation ; ite	
· ,··		.502	220.80	. A		06-1991	19321 1	ÿ JP₂ (· ; (EP ·	601 051	4018 6898	SA.0   A.3=	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	21-0	1-199	4
	US	537	3561	Α	13-1	12-1994	3 00	AU. AU	67 567	0166	B	11.5	04-0	7-199 7-199	6
Vi-	<u>!</u>	:				- 13° A	79/ N 10-131	> CA <sub>3</sub> 5	21/5 06/7	1590 6109	∂ <b>A</b> .,'C ::Α,:5		07-0 11-1	7-199 0-199	4 5
						ar yorl	. 3 na	WO.	5,944	5421	A m		07-0	7-199	4
•	US	563	8446	Α	10-0	6-1997	0 13(V	NONE	(9) L	366	25.5				_
		ŀ			C	1'ne 20		artaar Brian					•	•	
		1					•								
		!									•		1		
		•													
•													•	4	
													:		
													•		
														:	
		:											i	:	
		:													
		:													
													•		
		•													
														•	•
													į		1
		:											:		
		:											!		:
														,	ţ
													:		<b>1</b>
		;											1		:
		1		A .											

٠. :

. . .

REPORT OF STATE OF STATE

	, राष्ट्रकारकार राज्याचे हार प्राप्त हैं।	The Assembly of the	.1 .	SZELK:	
	Como de Resemblado e en 1992 a 199 COM about Rick Conception	1		Standard and the Control of the Cont	
The second of th					
	TO JOSEPH AND BEST REPORTED AND A SERVICE AN	: :::::	. Androis	grandade to the total about	
	or for Carbotta attractive todag or Solth LEM Devices of	1 7 20 Wy 20 War 1 2 2 2 2 2	2.18674.35	AND THE PROPERTY OF THE	
	i.dael.	on the second se		na on a restrictor	
	State and event from the total for any and the filler of the explanation of the event of the total control of the	2. Salasani 28.37 (10) 2. Salasani 28.37 (10) 78.0) (200) 201 (20) 2.002 (00) (20) (20) 2.002 (20) (20)	os nemili Lightav (190	er a fin Lingg († 1 – 11). 1801–1811 Medi G. M. Nath Champy (4).	

so the setting of the page BLANK (USPTO) be reflected to the control of the contr

11 (4.1) th moderation 11355 The second of 

19 4 6 150 10 11 15 15 15



#### WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau



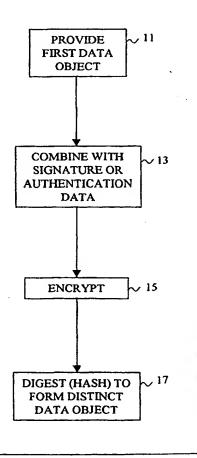
#### INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7: WO 00/13368 (11) International Publication Number: **A1** H04L 9/32 (43) International Publication Date: 9 March 2000 (09.03.00) : PCT/US99/18824 (81) Designated States: CA. IL. IN, JP. KR, MX, SG, European (21) International Application Number: patent (AT. BE, CH, CY. DE, DK, ES, FI, FR, GB, GR, IE, (22) International Filing Date: 27 August 1999 (27.08.99) IT, LU, MC, NL. PT. SE). Published (30) Priority Data: 09/144,043 31 August 1998 (31.08.98) US With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of (71)(72) Applicant and Inventor: BORGERS, Frederick, [US/US]; 105 Mill Valley, Colleyville, TX 76034 (US). (74) Agent: PERDUE, Mark, D.; Zisman Law Firm, 200 Renaissance Place, 714 Jackson, Dallas, TX 75202 (US).

#### (54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

#### (57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



1 mar 1 mar 2 mar 143 " 於 医隐肠病 食物医 177 CALIFORNIA LANGUAGO POR LANGUAG SOLUCION THE STATE OF THE STATE Sold that have been a second A JOSEPH CONTRACT STATES astronomic made also bear the first POLERSCOUNTS ne in Lewis Inc. Constitution (1998) iking nakag kanadakantaka / pizpadua nchi (53) AND THE ROOM OF ME MONEY FOR A SECTION OF BUTTOUR A COMPAND POWER TO SUPPREMENDED AND A SUPPREMENTATION OF THE COMPAND AND A SUPPREMENT MANG PERFERENCE FOR BRURBS BEET NOT FIRST CHARGE DITTER PROPERTY OF THE PRINCE SOCIETIES AND ELLECTRICES INFORMATIONS OF THE The second of th and the second of the second o The Salar glober Mission spiriter is to (34) Vertick War on Ennic (54) negetings most and an arms are stated and are seen as a second of the se Bu consiste that lite introduction to the second control of the se (इस्से नज्य कर्मा कर्मा कर्मा and the second of the second unsplacement of the land in House in Land of Francisco (Francisco) 🕏 人名 网络人的复数 经营制税的证券的 1. A. C.

FOR THE PURPOSES OF INFORMATION ONLY

The process of the control of the cont

THO THE SPANISH ON THE TANK OF THE WILL AS A STATE OF

1. 1E ( 0.41 N) (1.40N) (2003)

File of the Work State Car Car

CHESTORY PART CO. THE T

LYMAGES OF A CONTROL OF

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PC

Arm Was

性化 医原性结婚 活

# · · · · · · · ·

AL	Albania	ES	Spain	LS	Lesotho	0.		
AM	Armenia	FI	Finland	LT	Lithuania	SI	Slovenia	
AT	Austria	FR	France	· LU		SK	Slovakia	
AU.	Australia	GA	Gabon	LV	Luxembourg	SN	Senegal	
AZ	Azerbaijan	GB	United Kingdom	MC	Latvia	SZ	Swaziland	
BA	Bosnia and Herzegovina	GE	Georgia	1	Monaco	TD	Chad	
вв	Barbados	GH	Ghana	MD	Republic of Moldova	TG	Togo	
BE	Belgium	GN	Guinea	MG	Madagascar	TJ	Tajikistan	
BF	Burkina Faso	GR	Greece ·	MK	The former Yugoslav	TM	Turkmenistan	
BG	Bulgaria	HU		1	Republic of Macedonia	TR	Turkey	
ВJ	Benin	IE	Hungary Ireland	ML	Mali	TT	Trinidad and Toba	·go
BR	Brazil	IL	Israel	MN	Mongolia	UA	Ukraine	
BY	Belarus	IS	Iceland	: MR	Mauritania	UG	Uganda	
CA	Canada	IT		. MW	Malawi	US	United States of A	merica
CF	Central African Republic	JP	Italy	MX	Mexico	UZ	Uzbekistan	
CG	Congo	KE	Japan	NE	Niger	VN	Viet Nam	
СН	Switzerland	KG	Kenya	NL	Netherlands	YU	Yugoslavia	e-
CI	Côte d'Ivoire	KP	Kyrgyzstan	NO	Norway	ZW	Zimbabwe	_ !
CM	Cameroon	KP	Democratic People's	NZ	New Zealand			Ç.,
CN	China	· 7/10	Republic of Korea	PL	Poland			
CU	Cubaco equi servicio percenti	KK	Republic of Korea	PT.	Portugal Romania	g pr 150.	1.511.15.45.	
CZ	Czech Penublic	C. Com	Kazakstan	RO	Romania Russian Federation	ah	randa (Biba) 🕮	,
DE	Czech Republica a para de la Germany	LC	Saint Lucia: 1994 1994	N. RU	Russian Federation			
DK	Denmark	LL C	Liechtenstein at Yang and it	SD.	Sudan			٠.
EE	Estonia	LK `	Sri Lanka fra mand a		Sweden	· ::		
	Contra Co	LR	Liberia	SG.	Singapore			. '
			441 + 4V + 5	at v	.•			